Кафедра СУМГФ

ФК– 2024/2025 - занятия N13

Системы аудита безпасности и мониторинга Lynis и OpenSCAP

.

1. Обязательные процедуры при подключении к хосту перед началом работа (администрирования):

- зарегистрироваться на своем хосте

- выполнить команду **sudo bash** и получить права суперпользователя **root**   
- выполнить команду **w** для получения информации:  
В заголовке выводятся следующие поля:

* текущее время,
* время работы системы без перезагрузки (uptime),
* количество работающих в данный момент пользователей,
* среднее значение нагрузки системы за последние 1, 5 и 15 минут (Load averages).

В таблице для каждого пользователя выводятся следующие поля:

* USER — имя пользователя.
* TTY — название терминала.
* FROM — название удаленного компьютера или IP-адрес.
* LOGIN — время входа в систему.
* IDLE — время бездействия.
* JCPU — время, использованное всеми процессами, подключенными к tty. Оно не включает завершенные фоновые задания, но включает фоновые задания, работающие в данный момент.
* PCPU — время, использованное текущим процессом, который указан в поле WHAT.
* WHAT — текущий процесс (командная строка текущего процесса).

- выполнить команду **last -10** для уточнения кто регистрировался последние 10 раз **-** выполнить команду **top** и обратить внимание на возможную аномалию величины **load average** в первой строке вывода

для понимания нагрузки на хосте за последние 1, 5 и 15 минут  
- выполнить команду **free** для понимания наличия свободной памяти  
- выполнить команду **df -h** для понимание наличия свободного дискового пространства на разделах  
- выполнить команды **apt update, apt upgrade** и, при необходимости, **apt dist-upgrade** для обновления системы

1. Выбрать один из трех вариантов развертывания пакета Lynis:  
   А - установка с репозитария Debian  
   Б - установка с сайта разработчика   
   B - установка с репозитария Github

А. Для установки с репозитария Denian просто выполнить команду apt **install lynis**  
и проверить актуальность релиза пакета командой **lynis update info.** Обратить внимание на номер версии и год выпуска.  
  
Б. Для установки актуальной версии системы аудита, защищенности и соответствия Lynis установить зависимости:

**apt install wget curl gpg apt-transport-https**

- получить и установить ключ репозитария (из руководства с официального сайта <https://cisofy.com/>)

**curl -fsSL https://packages.cisofy.com/keys/cisofy-software-public.key | sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/cisofy-software-public.gpg**

- не скачивать другие языковые пакеты **Lynis**, кроме английского  
**echo 'Acquire::Languages "none";' | sudo tee /etc/apt/apt.conf.d/99disable-translations**

- добавить новый репозитарий в список **apt**  
**echo "deb https://packages.cisofy.com/community/lynis/deb/ stable main" | sudo tee /etc/apt/sources.list.d/cisofy-lynis.list**

- произвести обновление системы и установить актуальный релиз системы Lynis   
**apt update  
apt install lynis**

**-** проверить версию пакета и дату релиза

**lynis update info**

В. Установка с Github  
установить утилиту **git,** перейти в каталог, в который будет клонировал релиз Lynis, клонировать пакет и запустить программу  
**apt install -y git ; cd /usr/local/bin ; git clone https://github.com/CISOfy/lynis**

**cd lynis**

проверить версию пакета и дату релиза  
**lynis update info –** на мониторе должно быть примерно такое сообщение  
  
== Lynis ==

Version : 3.1.2

Status : Unknown

Release date : 2024-09-26

Project page : https://cisofy.com/lynis/

Source code : https://github.com/CISOfy/lynis

Latest package : https://packages.cisofy.com/

1. Выполнить сканирование систему и проанализировать отчет  
   **lynis audit system**В конце отчета будет приведен **Hardening index** и рекомендации по улучшению защиты.

Журнал (log) отчета находится в **/var/log/lynis.log**

Руководствуясь рекомендациями, попробовать улучшить индекс защиты.

1. Рассмотреть и понять положительные и отрицательные стороны вариантов А, Б и В.

----

Для развертывания сканера уязвимостей **OSCAP** и получения отчета в формате HTML установить необходимые пакеты, включая браузер, например, links2:  
**apt install openscap-scanner openscap-utils bzip2 links2**

1. Перейти в каталог **/root,** загрузить содержимое OVAL, предоставленное с официального ресурса <https://www.debian.org/security/oval/> и просканировать систему. Ознакомиться с датой и временем выпуска последней редакции архивного файла OVAL можно по ссылке <https://www.debian.org/security/oval/> . Обновление файла по этой ссылке происходит очень часто  
**cd /root ; wget https://www.debian.org/security/oval/oval-definitions-bookworm.xml.bz2**

2. Распаковать полученный файл   
**bzip2 -d oval-definitions-bookworm.xml.bz2**

3. Выполнить сканирование системы  
**oscap oval eval --report** *имя-вашего\_хоста***.html oval-definitions-bookworm.xml**где*имя-вашего\_хоста***.html,** например, **136.html (**от IP адреса хоста 192.168.10.136) . Можно также использовать функцию утилиты `date` для задания даты в имени файла отчета (см. предыдущие задания)

4. Просмотреть полученный отчет утилитой **mc (F3)** или браузером – **w3m, linx, links2** или скопировать в каталог ранее установленного на хосте http-сервера для доступа по сети. В этом случае необходимо ограничить доступ постронних лиц к страничке отчета по логину и паролю.  
**links2 *имя-вашего\_хоста*.html.**

5. Проанализировать полученный отчет и принять меры для устранения уязвимостей. Если обновление командой **apt upgrade** не устраняет уязвимости в системе, то необходимые компоненты можно скачать в каталог **/usr/src** с зеркала репозитария и инсталлировать вручную.   
**mc -> F9 -> Options > FTP link ->** [**ftp.ru.debian.org**](ftp://ftp.ru.debian.org) **-> debian > pool** – найти необходимый компонент и установить командой **dpkg -i *необходимый\_компонент*.deb**

6. Если сканирование системы произвоится регулярно, то необходимо предварительно удалить ранее полученный файл **oval-definitions-bookworm.xml.bz2** и и файлы отчета .xml, html

\*Файл этого задания можно получить на облачном сервисе кафедры в каталоге дата\_занятия по ссылке <https://bombey.mipt.ru/>

**логин student-308 пароль 76XxKLws-2024**